REMARKS

This Amendment is in response to the Final Office Action dated June 29, 2005. In the Office Action, claims 7-8, 24, 25, 30-33, and 35 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 25 is further rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1-3, 9, 11, 15, 17, 22, and 26 were rejected under 35 U.S.C. § 102(e) as being anticipated by Devine et al., U.S. Patent No. 6,397,242 (hereinafter *Devine*). Claims 21 and 23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Devine* as applied to claims 1 and 2, respectively, in view of "Extensible Firmware Interface Specification Version 1.02" by Intel Corporation (hereinafter *Intel*). Claims 7, 8, 24, and 25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Devine* in view of *Intel*. Claims 33 and 34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Devine* as applied to claim 9 in view of *Intel*. Claim 37 was rejected under 35 U.S.C. § 103(a) as being unpatentable over *Devine* as applied to claim 15 above, and further in view of *Intel*.

Allowable Subject Matter

Claims 27-29 would be allowable if rewritten or amended to overcome the rejections under 35 U.S.C. § 112, second paragraph and 35 U.S.C. § 101, set forth in the Office Action. Claims 30-32 and 35 would be allowable if rewritten or amended to overcome the rejections under 35 U.S.C. § 112, second paragraph set forth in the Office Action, and rewritten in independent form including all of the limitations of the base claim and any intervening claims. The allowable status of these claims depends on the manner in which the rejections under 35 U.S.C. § 112, second paragraph are resolved.

Claims 9, 11, 15, 17, 27, 29, and 32 are amended as shown above. Specifically, independent claims 9, 15, and 27 are amended to overcome the 35 U.S.C. § 112, second paragraph and 35 U.S.C. § 101 rejections discussed above. Claims 1-8, 10, 12-14, 16, 18-26, 28, 30, 31, and 33-36 are canceled herein without prejudice. Thus, claims 9, 11, 15, 17, 27, 29, 32, and 37 are now pending in the application. For the reasons set forth below, the Applicants respectfully request reconsideration and allowance of all pending claims.

Argument in Support of Allowance of the Amended Claims

Each of independent claims 9, 15, and 27 have been amended herein to overcome their respective 35 U.S.C. § 112, second paragraph and 35 U.S.C. § 101 rejections, and to incorporate allowable subject matter identified above. More specifically, claim 9 now recites,

9. A machine-readable medium that provides executable firmware instructions which, when executed by a processor in a computer system having a native environment that executes in physical mode, cause the processor to perform operations comprising:

implementing an extensible firmware framework via which firmware modules are loaded during a pre-boot phase of the computer system

implementing a firmware-based virtual machine monitor (VMM) upon the computing system;

emulating legacy hardware components that are not present in the native environment using the VMM to provide support for legacy code running on the computer system; and

authenticating, via the VMM, a firmware module that is loaded during the pre-boot phase by comparing a digital signature provided with the firmware module with digital signatures stored in secure storage that is accessible to the VMM.

The term "third-party" firmware modules has been removed to address the 35 U.S.C. § 112, second paragraph issue. The limitation of "authenticating a firmware module via the VMM by comparing a digital signature provided with the firmware module with digital signatures stored in secure storage that is accessible to the VMM" was previously recited in dependent claim 31 (now cancelled), which, as discussed above, contained allowable subject matter.

Similarly, claim 15 has been amended to incorporate the allowable subject matter of objected-to claim 36 and to overcome the 35 U.S.C. § 112, second paragraph issue, and now recites,

15. An apparatus comprising:

a computing system having a native execution environment that executes in physical mode, the computer system including an extensible firmware framework via which firmware modules are loaded during a pre-boot phase of the computer system; and

a virtual machine monitor implemented thereon, the virtual machine monitor emulating legacy hardware components that are not present in the native environment to provide support for legacy code to run on the computer system, the virtual machine monitor further authenticating a firmware module loaded during the pre-boot phase by comparing a digital signature provided with the firmware module with digital signatures stored in secure storage accessible to the VMM.

Finally, claim 27 has been amended to include the allowable subject matter of claim 28.

Conclusion

Overall, none of the references singly or in any motivated combination disclose, teach, or suggest what is recited in the independent claims. Thus, given the above amendments and accompanying remarks, independent claims 9, 15, and 27 are now in condition for allowance. The dependent claims that depend directly or indirectly on

these independent claims are likewise allowable based on at least the same reasons and based on the recitations contained in each dependent claim.

If the undersigned attorney has overlooked a teaching in any of the cited references that is relevant to the allowability of the claims, the Examiner is requested to specifically point out where such teaching may be found. Further, if there are any informalities or questions that can be addressed via telephone, the Examiner is encouraged to contact the undersigned attorney at (206) 292-8600.

Charge Deposit Account

Please charge our Deposit Account No. 02-2666 for any additional fee(s) that may be due in this matter, and please credit the same deposit account for any overpayment.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Date: Oct 14 2005

R. Alan Burnett
Reg. No. 46,149

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1030